PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/16

A1

(11) International Publication Number: **WO 99/30499**

(43) International Publication Date: 17 June 1999 (17.06.99)

(21) International Application Number: PCT/US98/26296

(22) International Filing Date: 10 December 1998 (10.12.98)

(30) Priority Data:

60/069,090	10 December 1997 (10.12.97)	US
60/086,567	21 May 1998 (21.05.98)	US

(71) Applicant *(for all designated States except US)*: THOMSON CONSUMER ELECTRONICS, INC. [US/US]; 10330 North Meridian Street, Indianapolis, IN 46290–1024 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: ESKICIOGLU, Ahmet, Mursit [–/US]; 8235 Lakeshore Trail # 125, Indianapolis, IN 46250 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; GE & RCA Licensing Management Operation, Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

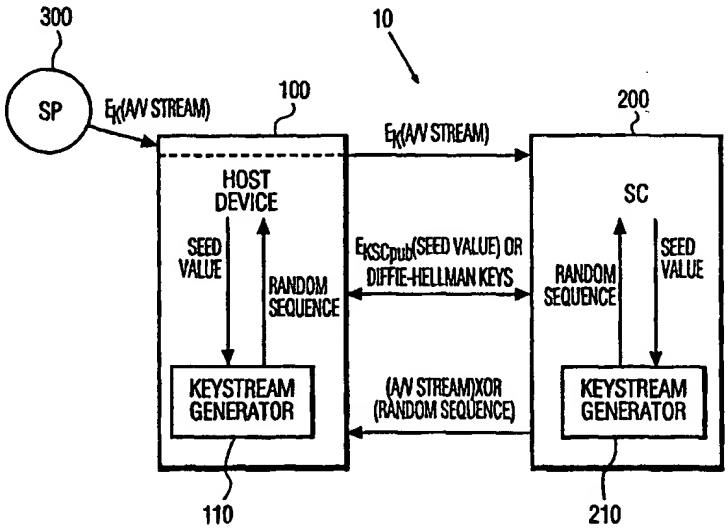
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR PROTECTING THE AUDIO/VISUAL DATA ACROSS THE NRSS INTE RFACE



(57) Abstract

A system for enhancing the security of the interface between a consumer electronic device and a removable security device is provided by protecting the audio/visual (A/V) stream descrambled in the removable security device. The protection involves dynamically computing a shared key followed by the rescrambling of the A/V stream.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD FOR PROTECTING THE AUDIO/VISUAL DATA ACROSS THE NRSS INTERFACE

Field of the Invention

This invention concerns a system for enhancing the security of the interface between a consumer electronic device and a removable security device such as the interface defined by the National Renewable Security Standard (NRSS). Security is enhanced by protecting the audio/visual (A/V) stream that is descrambled by the removable security device, such as a smart card, coupled to the consumer electronic device. Examples of consumer electronic devices employing the NRSS smart cards include digital television receivers, digital video cassette recorders as well as separate devices or "boxes" that may be located on top of, or coupled to, a television receiver, i.e., set-top boxes.

Background of the Invention

A concern of today's emerging digital consumer electronic products is the ability to access a plaintext (i.e., in-the-clear) digital bitstream thereby permitting one to make unauthorized digital copies of the bitstream. The National Renewable Security Standard (NRSS) (EIA-679) developed by the Electronic Industries Alliance provides a means for employing renewable security in connection with digital consumer electronics (CE) devices, for example, digital television receivers, digital video cassette recorders and set-top boxes. Renewable security allows for the development of conditional access systems that can be replaced, upgraded or recovered with minimum cost and effort.

Typically, a service provider will scramble (or encrypt) the signal before it is transmitted or broadcast. A conditional access (CA) device (e.g., an NRSS smart card) may be used to descramble (or decrypt) the signal and route it to the host device. However, a problem with the NRSS architecture is that the audio/visual (A/V) stream is sent to the host device (for example, a display device or a set top box) from the smart card in-the-clear. That is, the A/V

stream is not scrambled when it leaves the CA device. Thus a person can monitor this line and use a data capturing device to record all the data.

Summary of the Invention

This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem. Generally, the present invention defines a method for protecting the output audio/visual (A/V) stream of a smart card by receiving a scrambled signal from a source external to said smart card, generating a descrambling key in response to said received signal, descrambling said received signal using said descrambling key to generate a descrambled signal, receiving data from said external source, generating a scrambling key in response to said received data, scrambling said descrambled signal using said scrambling key to generate a rescrambled signal, providing said rescrambled signal to said external source.

In accordance with one aspect of the present the received data is a scrambling key encrypted using a public key associated with said smart card and wherein the step of generating said scrambling key comprises decrypting said encrypted scrambling key using a private key associated with said smart card, said private key being stored in said smart card.

In accordance with one aspect of the present invention, the scrambling key comprises a seed value and the step of scrambling the descrambled signal generating a random sequence in response to the seed value, and generating the rescrambled signal by exclusive ORing said random sequence and said descrambled signal.

In accordance with another aspect of the present invention, the received scrambled signal comprises video, audio and control packets and the seed value is generated, in the external source, in a unique manner in response to said video, audio and control packets.

In accordance with another aspect of the present invention, the smart card verifies the seed value by comparing the seed value to a subsequent seed value generated in the unique manner in response to the video, audio and control packets.

In accordance with yet another aspect of the present invention, the seed value is generated utilizing one of the hash of video, audio and control packets or by exclusive ORing said video, audio and control packets together.

In accordance with yet aspect of the present invention, a first seed value is generated in the smart card and the received data is a second seed value. The step of generating said scrambling key comprises generating said scrambling key in response to said first and second seed values.

In accordance with yet aspect of the present invention, a system for managing access between a service provider and a host device having a smart card coupled is provided. The host device performing the steps of: receiving a scrambled signal from the service provider, sending, to the smart card, a seed value generated in the host device and encrypted using a public key of the smart card, coupling the received signal to the smart card, and receiving from the smart card the rescrambled signal. The smart card has a means for access control processing, comprising means for generating a descrambling key in response to the received signal, means for descrambling the received signal using the descrambling key to generate a descrambled signal, means for decrypting the encrypted seed value using a private key of the smart card to provide the seed value, means for generating a random sequence in response to the seed value and means for scrambling the descrambled signal using the random sequence and the descrambled signal to generate a rescrambled signal.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawings

Figure 1 is a block diagram of an exemplary implementation of a system for enhancing the security of the interface between a consumer electronic device and a renewable security device in accordance with the invention; and

Figure 2 is a schematic block diagram illustrating the signal flow of Figure 1.

Detailed Description of the Drawings

When a conditional access (CA) device (or a smart card (SC)) receives a transmitted or broadcast signal (i.e., a program or event) that is scrambled (or encrypted), the CA device may be used to descramble (or decrypt) the signal. The National Renewable Security Standard (NRSS) provides a means for implementing renewable security in connection with smart cards employed with digital consumer electronics (CE) devices, such as, digital television receivers (DTV), digital video cassette recorders (DVCR) and separate devices or "boxes" that may be located on top of, or coupled to, a television receiver, i.e., set-top boxes (STB). A potential problem with the NRSS architecture is that the audio/visual (A/V) stream is not scrambled when it leaves the smart card. This provides a point in which the security of the CA system could be breached because one could monitor and tap the output of the smart card and use a data capturing device to record all the plaintext data. The present invention provides an improvement to protect the connection between the smart card and the CE device. Such smart cards include ISO 7816 cards having a card body with a plurality of terminals arranged on a surface in compliance with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B.

In Figure 1, a system 10 for protecting the A/V stream of CE device 100 which employs NRSS smart card (SC) 200 is depicted. Such CE or host devices 100 include DTVs, DVCRs or STBs. Smart Card 200 is inserted into, or coupled to, a smart card reader 105 included in, or coupled to, host device 100; bus 150, internal to host device

100, interconnects host device 100 and SC 200 thereby permitting the transfer of data therebetween. Host device 100 is connected to a cable, satellite or broadcast service provider (SP) 300 via a link 350. The protection system of the present invention will be described in relation to system 10 as shown in Figures 1 and 2.

For the protection of the NRSS interface (i.e., the return path), A/V data processing in accordance with this invention include rescrambling the plaintext A/V data in the smart card. A requirement of consumer electronic manufacturers for the design of a CA system is to avoid the permanent storage of any secrets in the host device. Thus, the rescrambling key cannot be exchanged using an architecture where a private or a shared secret key is embedded in the host. The rescrambling key should be dynamically established without modifying the present smart card architecture drastically. A dynamic key is one that is generated on-the-fly in real-time and is not fixed. Periodic (for example, every ten seconds) generation of new keys is normally needed to increase the robustness against cryptanalytic attacks.

Two key establishment protocols can be considered for this purpose:

1) A key transport protocol (e.g., public-key encryption): One party creates the key to be shared, and securely sends it to the other.

2) A key agreement protocol (e.g., Diffie-Hellman): The shared key is derived by two parties as a function of data contributed by each of them.

The key that is shared between the smart card and the host can be used in a number of ways to scramble the A/V stream before it is sent back to the host. For example, block ciphers may be considered for rescrambling. Since the DES algorithm is typically used for descrambling the incoming A/V stream, it could be used for rescrambling the signal. However, such a complex cipher engine in the host device would increase the manufacturing cost and complexity.

Synchronous stream ciphers are appropriate for rescrambling. A synchronous stream cipher is one in which the key stream is generated independently of the plaintext and ciphertext messages. Although the design of most practical stream ciphers is centered around linear feedback shift registers (LFSRs) (because they are well-suited for hardware implementations, produce sequences with large periods and good statistical properties and are amenable for analysis), there is a variety of other approaches.

The key generator 110 can be initialized with the shared key to obtain the random sequence. The frequency of renewing the seed is an implementation dependent parameter. The seed will, in general, be different for each renewal, thus resulting in dissimilar random sequences for discouraging cryptanalytic attacks. The general architecture of such a system is shown in Figure 2.

Particularly, this invention, in one embodiment, provides for the dynamic generation of a key within the host device 100 utilizing an RSA (Rivest, Shamir and Adelman) engine. This key is shared with SC 200 and is used to rescramble the audio/visual (A/V) stream prior to it leaving the SC 200. Both the host device 100 and SC 200 contain RSA engines for encryption and decryption. An RSA engine may be implemented using a co-processor (i.e. a microprocessor). Since the public key of the smart card is available to the host device as well as to the service providers, it can be used by the host to encrypt a scrambling key before it is sent to the smart card.

The protocol using the RSA public key system involves the encryption of the dynamic key in host device 100 using the public key of smart card 200. The encrypted dynamic key is transmitted to smart card 200 and is decrypted using the private key of the smart card. This is an asymmetric key system, wherein only public keys are stored in the STB or DTV or DVCR. That is, the device does not store or contain any secrets (i.e., private keys). The foundation of public-key cryptography is the use of two related keys, one public and one private; the private key being computationally unfeasible of being deduced from the public key which is publicly available.

Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can decrypt it.

In another embodiment of the present invention, both host device 100 and SC 200 have Diffie-Hellman engines to generate a shared key. Neither host device 100 nor SC 200 can alone generate the key. A first seed value generated in SC 200 is sent to host device 100 and a second seed value generated in host device 100 is sent to SC 200. Together, host device 100 and SC 200 generate the shared key.

Both of the key establishment protocols are subject to attacks if the host device participating in the key generation is not authenticated. An improvement is possible by generating the shared seed as a function of the transport stream transmitted to the card in an initial time period. As the audio/video packets are scrambled, and the Entitlement Control Messages (ECMs) are encrypted, they can be used as functional arguments. This can provide implicit key authentication.

For example, if both host device 100 and smart card 200 have RSA engines, and the host has a copy of the card's public key, K_{pubSC}, the host can construct the seed using a function of the video, audio, and ECM packets:

Shared seed: (random number | f(A, V, ECM))

As an another example, if both host device 100 and smart card 200 have Diffie-Hellman engines and they exchange the keys α^x and α^x, the exponent x can be constructed using a function of the video, audio and ECM packets:

$(\alpha^{\text{random number}}, \alpha^{f(A,V,ECM)})$, where x=(random number + f(A,V,ECM)

In both examples, the smart card 100 computes the same functional value independently and compares it with that sent by the

host. This effectively provides host authentication, preventing the intruders from impersonating the host.

The function f = f(A, V, ECM) can be defined in a number of ways. Two possible definitions are:

1) f = hash (A, V, ECM)
2) f = A xor V xor ECM

Note that these definitions may include more than three packets. The number and positions of the A, V, and ECM packets in the stream are also a part of the function definition.

A one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) may be used to determine the hash function "f".

For more security, the seed needs to be renewed periodically. Renewal is possible by recomputing the function for each time interval. For example, the first packet encountered in each of the A, V, and ECM substreams in every 30 seconds can be used in generating a new key stream for scrambling. Alternatively, packets can be numbered for synchronization between the host and the card.

Generation of the shared seed as a function of the transport stream makes the attacks on the proposed key establishment protocols more difficult. This does not require additional cryptographic tools. As the transport stream is shared by the host and the card, it can be used with minimal computation to implicitly authenticate the host.

This invention provides protection against copying of copyrighted A/V streams in transmission to the host. The modified key establishment protocols can be used to prevent active attacks. Thus, if the key is defined to be a function of the MPEG-2 transport stream (i.e., service packets and ECMs), the hacker would also need to access the stream and extract the required data out of it.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon a reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims.

CLAIMS

1. A method for protecting the output audio/visual stream of a smart card comprises the steps of:

(a) receiving a scrambled signal from a source external to said smart card;

(b) generating a descrambling key in response to said received signal;

(c) descrambling said received signal using said descrambling key to generate a descrambled signal;

(d) receiving data from said external source;

(e) generating a scrambling key in response to said received data;

(f) scrambling said descrambled signal using said scrambling key to generate a rescrambled signal.

(g) providing said rescrambled signal to said external source.

2. The method of Claim 1 wherein said received data is a scrambling key encrypted using a public key associated with said smart card and wherein the step of generating said scrambling key comprises decrypting said encrypted scrambling key using a private key associated with said smart card, said private key being stored in said smart card.

3. The method of Claim 2 wherein said scrambling key comprises a seed value and wherein the step of scrambling said descrambled signal comprises the steps of:

(a) generating a random sequence in response to said seed value; and

(b) generating said rescrambled signal by exclusive ORing said random sequence and said descrambled signal.

4. The method of Claim 3 wherein said received scrambled signal comprises video, audio and control packets and said seed value is generated, in said external source, in a unique manner in response to said video, audio and control packets.

5. The method of Claim 4 wherein said smart card verifies said seed value by comparing said seed value to a subsequent seed value generated in said unique manner in response to said video, audio and control packets.

6. The method of Claim 5 wherein said seed value is generated utilizing said hash of video, audio and control packets.

7. The method of Claim 5 wherein said seed value is generated by exclusive ORing said video, audio and control packets together.

8. The method of Claim 1 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

9. The method of Claim 1 further comprising the step of generating, in said smart card, a first seed value, and wherein said received data is a second seed value.

10. The method of Claim 9 wherein the step of generating said scrambling key comprises generating said scrambling key in response to said first and second seed values.

11. The method of Claim 10 wherein said scrambling key comprises a seed value and wherein the step of scrambling said descrambled signal comprises the steps of:

(a) generating a random sequence in response to said seed value; and

(b) generating said rescrambled signal by exclusive ORing said random sequence and said descrambled signal.

12. The method of Claim 11 wherein said received scrambled signal comprises video, audio and control packets and said first and second seed values are generated in a unique manner in response to said video, audio and control packets.

13. The method of Claim 10 wherein said first and second seed values are generated utilizing said hash of video, audio and control packets.

14. The combination of Claim 10 wherein said first and second seed values are generated by exclusive ORing said video, audio and control packets together.

15. A system for managing access between a service provider and a host device having a smart card coupled thereto, said host device performing the steps of:

(a) receiving a scrambled signal from said service provider;

(b) sending, to said smart card, a seed value generated in said host device and encrypted using a public key of said smart card;

(c) coupling said received signal to said smart card, said smart card having a means for access control processing, said access control processing means comprising means for generating a descrambling key in response to said received signal, means for descrambling said received signal using said descrambling key to generate a descrambled signal, means for decrypting said encrypted seed value using a private key of said smart card to provide said seed value, means for generating a random sequence in response to said seed value and means for scrambling said descrambled signal using said random sequence and said descrambled signal to generate a rescrambled signal; and

(d) receiving from said smart card said rescrambled signal.

16. The system of Claim 15 wherein said public key is stored in said host device and said private key is stored in said smart card.

17. The system of Claim 16 wherein said host device is one of a digital television, a digital video cassette recorder and a digital set-top box.

18. A system for managing access between a service provider and a host device having a smart card coupled thereto, said host device performing the steps of:

(a) receiving a scrambled signal from said service provider;

(b) sending, to said smart card, a second seed value;

(c) coupling said received signal to said smart card, said smart card having a means for access control processing, said access control processing means comprising means for generating a descrambling key in response to said received signal, means for descrambling said received signal using said descrambling key to generate a descrambled signal, means for generating a first seed value, means for generating a scrambling key in response to said first and second seed values, and means for scrambling said descrambled signal using said scrambling key to generate a rescrambled signal; and

(d) receiving from said smart card said rescrambled signal.

19. The system of Claim 18 wherein said host device is one of a digital television, a digital video cassette recorder and a digital set-top box.

1/1

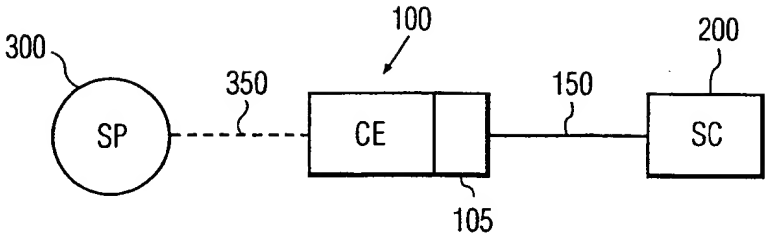

300
SP
350
100
CE
105
150
200
SC

FIG. 1

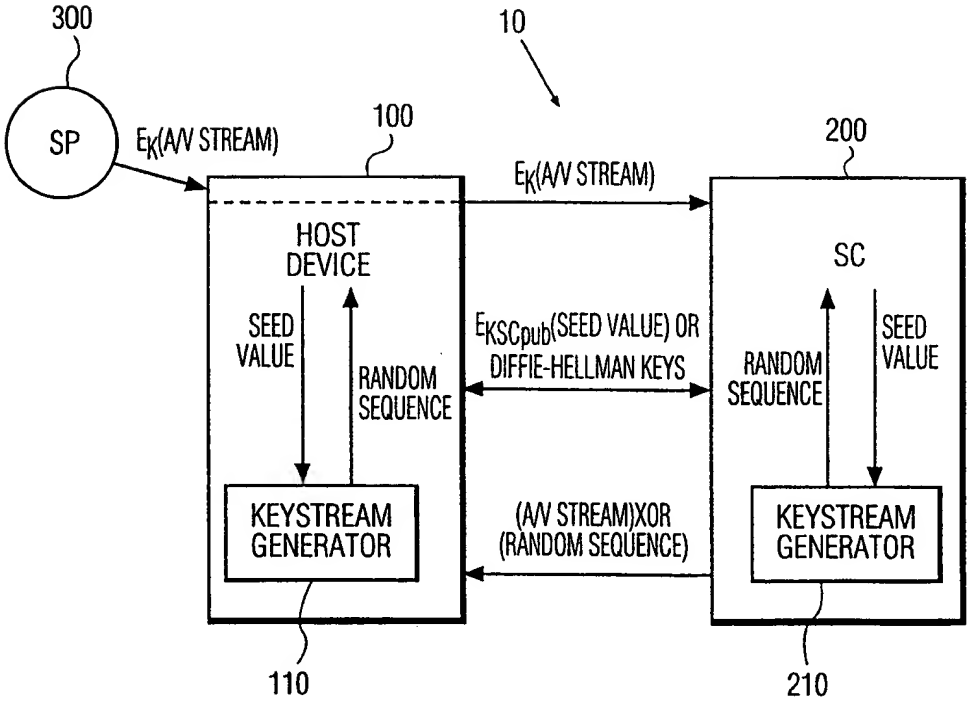

300
SP
E_K(A/V STREAM)
10
100
HOST DEVICE
SEED VALUE
RANDOM SEQUENCE
KEYSTREAM GENERATOR
110
E_K(A/V STREAM)
E_{KSCpub}(SEED VALUE) OR DIFFIE-HELLMAN KEYS
(A/V STREAM)XOR (RANDOM SEQUENCE)
200
SC
RANDOM SEQUENCE
SEED VALUE
KEYSTREAM GENERATOR
210

FIG. 2

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/US 98/26296

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 658 054 A (NEWS DATACOM LTD) 14 June 1995 see page 4, column 5, line 47 - column 6, line 47 see page 5, column 7, line 4 - line 25 see page 5, column 8, line 9 - page 6, column 9, line 38 see figures 2,3,5,6 ---	1,2,15, 16,18
A	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 see page 3, line 25 - page 4, line 5 see page 12, line 16 - page 13, line 7 see page 15, line 17 - page 17, line 6 see figures 1,4 --- -/--	1-5, 8-13,15, 16,18

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 April 1999	28/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. tional Application No
PCT/US 98/26296

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 714 204 A (LG ELECTRONICS INC) 29 May 1996 see page 6, line 11 - page 7, line 16 see figures 7-11	1,2, 15-19
A	SCHOONEVELD VAN D: "STANDARDIZATION OF CONDITIONAL ACCESS SYSTEMS FOR DIGITAL PAY TELEVISION" PHILIPS JOURNAL OF RESEARCH, vol. 50, no. 1/02, July 1996, pages 217-225, XP000627672 Hilversum, NL	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inta Jonal Application No
PCT/US 98/26296

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0658054 A	14-06-1995	IL	107967 A	05-12-1996
		AT	171331 T	15-10-1998
		AU	684112 B	04-12-1997
		AU	8034294 A	15-06-1995
		CA	2137608 A	10-06-1995
		DE	69413361 D	22-10-1998
		JP	7288522 A	31-10-1995
		US	5590200 A	31-12-1996
WO 9606504 A	29-02-1996	AU	3238595 A	22-03-1996
		AU	701593 B	04-02-1999
		AU	3239495 A	14-03-1996
		BR	9508621 A	30-09-1997
		BR	9508622 A	19-05-1998
		CA	2196406 A	07-03-1996
		CA	2196407 A	29-02-1996
		CN	1158202 A	27-08-1997
		CN	1158203 A	27-08-1997
		EP	0878088 A	18-11-1998
		EP	0782807 A	09-07-1997
		FI	970677 A	18-02-1997
		JP	10506507 T	23-06-1998
		JP	10505720 T	02-06-1998
		PL	318647 A	07-07-1997
		WO	9607267 A	07-03-1996
EP 0714204 A	29-05-1996	CN	1137723 A	11-12-1996
		JP	8242438 A	17-09-1996
		US	5757909 A	26-05-1998